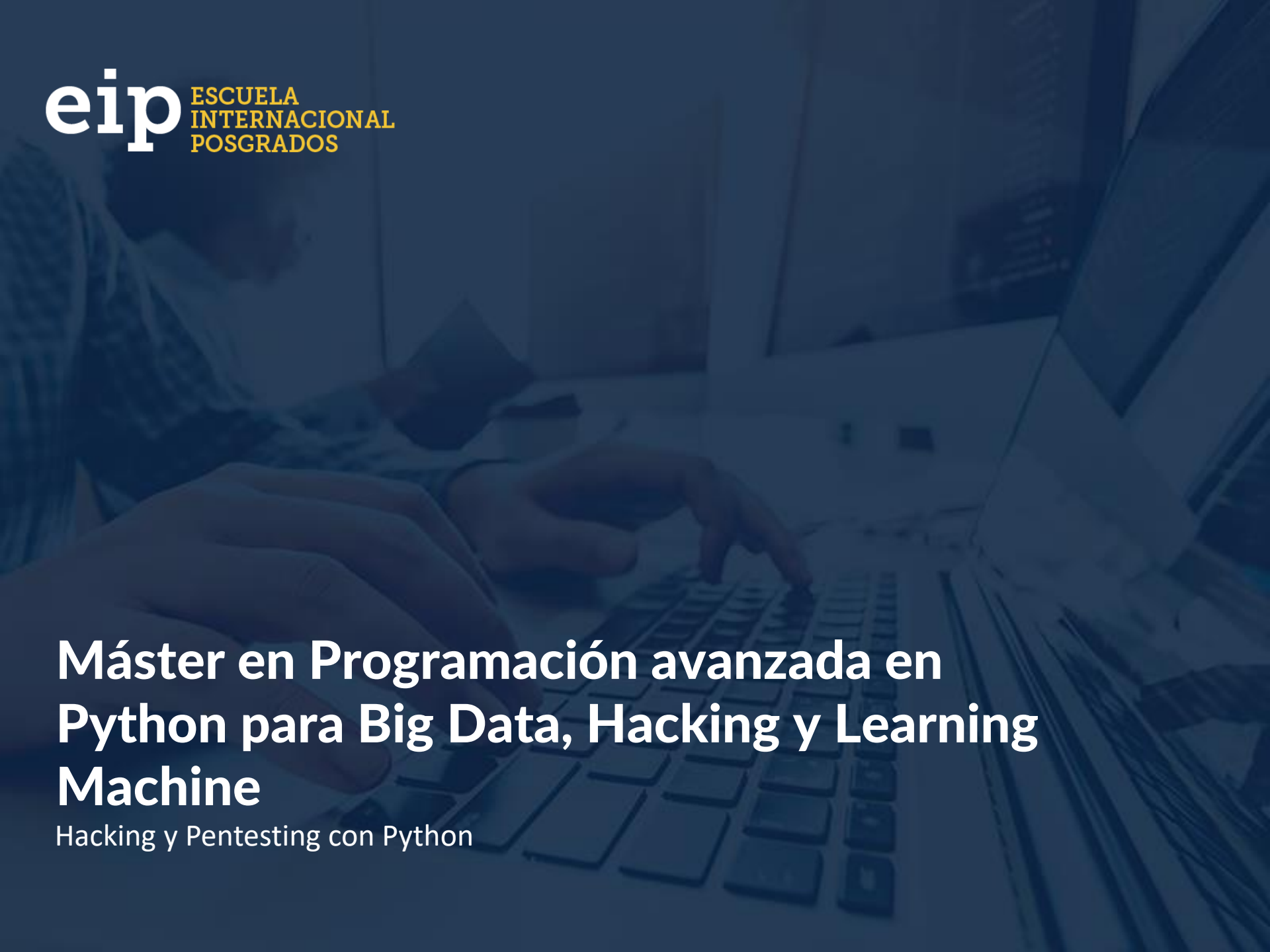

ESCUELA INTERNACIONAL POSGRADOS

Máster en Programación avanzada en Python para Big Data, Hacking y Learning Machine

Hacking y Pentesting con Python

MÓDULO 06

Creación de utilidades y herramientas para hacking ético.

Implementación de Bind y Reverse Shells

Desde un sistema comprometido un atacante puede instalar software y cualquier tipo de componente que le permita realizar pruebas de pentesting desde dicho sistema. Dichos componentes, entre otras cosas pueden establecer conexiones al sistema del atacante y enviarle una shell en el sistema comprometido. Esto se conoce como “reverse shell”. Por otro lado, también es posible abrir un puerto en la máquina comprometida y todo el tráfico entrante por dicho puerto le permitirá al atacante ejecutar comandos sobre el sistema comprometido. Esto se conoce como “bind shell”.

Las herramientas a instalar le permitirán al atacante aplicar técnicas de pivoting y port-forwarding con el fin de controlar las conexiones que realizará la máquina comprometida contra otros sistemas en otros segmentos de red que no estarán accesibles de forma directa para el atacante. El atacante puede llevar a cabo procesos de pentesting completos contra servicios específicos en los sistemas descubiertos en la red de la víctima.

Cracking de Hashes en sistemas Windows y Linux

Un hash representan una cadena de texto reducida que identifica de forma única a otro texto de tamaño mucho más amplio. Las funciones de hashing se utilizan en el mundo de la seguridad informática en múltiples escenarios dados sus beneficios.

En los sistemas operativos Windows y Linux, las credenciales se todos los usuarios no se almacenan en texto plano, en su lugar se utilizan algoritmos de hashing para almacenar esa representación de las contraseñas. Se trata de un mecanismo seguro que impide que cualquiera, aunque tenga permisos de administrador, pueda acceder a las credenciales en texto plano de cualquier usuario.

En sistemas basados en Unix, los algoritmos de hashing más comunes son MD5 y SHA2, sin embargo en el caso de sistemas Windows el algoritmo utilizado es NTLM.

MUCHAS GRACIAS POR SU ATENCIÓN

eip ESCUELA INTERNACIONAL POSGRADOS

decheverri@grupomainjobs.com

LINKEDIN

Daniel Echeverri
https://www.linkedin.com/in/adastra1/

twitter.com/eiposgrados

facebook.com/eiposgrados

instagram.com/eiposgrados